Symantec AntiVirus™ Command Line Scanner

Featuring Symantec AntiVirus™ technology

Symantec AntiVirus™ Command Line Scanner

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.0

Copyright Notice

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. CarrierScan Server, Bloodhound, LiveUpdate, NAVEX, Symantec AntiVirus, and Symantec AntiVirus Research Center (SARC) are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

CONTENTS

Symantec AntiVirus Command Line Scanner

Service and support solutions

CD Replacement Form

Symantec AntiVirus Command Line Scanner

The Symantec AntiVirus Command Line Scanner is a multi-platform utility that works in conjunction with an already installed CarrierScan Server running on the Windows NT/2000, Solaris, or Linux platforms.

Using the Command-line scanner

The Symantec AntiVirus Command Line Scanner lets you send files to a CarrierScan Server to be scanned for viruses. You can also initiate a scan of files located on the CarrierScan Server itself. Other features include the following:

- Repair infected files.
- Recurse subdirectories.
- Log command-line scanner operation.
- Exclude specified files or directories from scans.

The Symantec AntiVirus Command Line Scanner displays a text-based progress indicator to show activity. When the indicator pauses, a large file is likely being sent to the CarrierScan Server. An “e” in the display indicates that an error occurred. The progress indicator is displayed even if output is being captured to a log file.

Installation

The Symantec AntiVirus Command Line Scanner can reside on the same or a different computer as the CarrierScan Server. CarrierScan Server has been tested for the following platforms:

- Windows NT Server 4.0 or Windows 2000 Server
- Solaris 2.6 or higher
- Red Hat Linux version 6.2 or 7.1

Separate Symantec AntiVirus Command Line Scanner executables are provided for the Windows NT/2000, Solaris, and Linux platforms.

To install the Symantec AntiVirus Command Line Scanner, copy the following two files to any directory:

- cmdline (the operating system appropriate version)
- cmdline.cfg

The Symantec AntiVirus Command Line Scanner and the CarrierScan Server can be installed to different operating systems on different computers.

Syntax

cscmdline [options] <path> [<path>...]

<path>	What to scan: A file or directory. You can specify any mounted file system, mount point, or mapped drive. If the file or directory name contains spaces, you must enclose it in quotation marks (for example, “C:\Program Files”). The trailing * wildcard is supported for file names (for example, C:\Work\Dev*).
-a scan|repair	Action to take on infected file: scan or repair. If -a is omitted, Symantec AntiVirus Command Line Scanner repairs infected files by default.

-c <path>	Configuration file. If -c <path> is specified, it is used instead of the cscmdline.cfg file in the same directory as the cscmdline executable. If the file name or path contains spaces, use quotation marks. For example: cscmdline -c "C:\Program Files\myconfig.cfg" C:\Work
-i <n>	Information detail level: 0, 1, 2, 3, or 4 (least detail to most detail). If -i is omitted, cscmdline reports level 0 by default.
-f <path>	File for logging. If used, you must specify the file name. Without a path, the log file is written to the same directory as Symantec AntiVirus Command Line Scanner. Log entries are appended to an existing file. If the file name or path contains spaces, it must be enclosed in quotation marks (for example, "C:\Program Files\cscan.log").
-h	Help with command-line syntax.
-l	Located on the server. Files to scan are located on the CarrierScan Server itself. For cross-platform usage, the <path> file specification must be in the format of the operating system where the CarrierScan Server is installed. Use quotation marks to ensure that the file specification is passed properly. For example, if Symantec AntiVirus Command Line Scanner is running under Windows and the CarrierScan Server is running under Solaris: cscmdline -l -s 192.168.0.1 "/tim/export/jump.cmd" Recursion (-r option), directories, and wildcards are not supported if the CarrierScan Server is located on a different computer. In this case, you must specify full paths to explicitly named files for the <path> parameter.
-r	Recursive subdirectory scanning.

-s <IP address>[:<port>]	Server IP address and port of the CarrierScan Server. This option can be omitted if the CarrierScan Server is on the same computer as Symantec AntiVirus Command Line Scanner. You must specify the IP address and port if the CarrierScan Server is installed on a port other than the default (7777).
-v	Verbose output mode, if a virus is detected.

What to scan

<path>

The <path> parameter indicates one or more files or directories to scan, separated by spaces. You can specify any mounted file system, mount point, or mapped drive. For example:

```
C:\Work\Scantest.exe
/tim/export/home/jump.cmd
```

Because files are actually sent to the CarrierScan Server for scanning, you can only specify files or directories to which you have access permissions.

Note: With the -l option (Located on CarrierScan Server), only filenames are sent, not the files themselves.You can specify any filenames on the CarrierScan Server, irrespective of permissions.

If the file or directory name contains spaces, it must be enclosed in quotes. For example:

```
"C:\Program Files"
```

The trailing * wildcard can be used. For example:

```
C:\Work\Dev*
C:\Work\*
```

To scan descending subdirectories, include the -r option (Recursive subdirectory scanning). For example:

```
cscmdline -s 192.168.0.100 -r d:\
```

There is a small usage anomaly when recursively scanning from the root of a drive of Win32 computers. For Windows 95, 98, and Me, the * wildcard must be specified. For example:

```
cscmdline -s 192.168.0.100 -r d:\*
```

For Windows NT/2000, the * wildcard can either be specified or omitted.

```
cscmdline -s localhost -r d:\
```

-a scan|repair

Action to take on infected file.

If the -a option is omitted, cscmdline repairs infected files by default. For example:

```
cscmdline -s 192.168.0.100 c:\winnt
```

If you only want files scanned and not repaired, you must specify -a scan on the command line. For example:

```
cscmdline -s 192.168.0.100 -a scan c:\winnt
```

Configuration file for exclusions

-c <path>

To reduce demand on network resources, the configuration file lists files and directories to exclude from scans. Items not at risk of infection can be skipped.

If -c <filename> is specified, it is used instead of the cscmdline.cfg configuration file that is located in the same directory as the cscmdline executable. For example:

```
cscmdline -s 192.168.0.1 -c myconfig.cfg  -r c:\
```

See “Configuration file options” on page 14 for information about excluding files from scans.

Note: If cscmdline.cfg does not reside in the same directory as the cscmdline executable, a configuration file must be specified with the -c <filename> option.

File for logging

-f <path>

By default, no log file is created for a Symantec AntiVirus Command Line Scanner operation. To create a log file, specify the -f option with the log filename. For example:

```
cscmdline -s 192.168.0.100 -f c:\cmdline.log c:\winnt
```

Data is appended to an existing log file. If a log file is specified, only progress is reported on screen. All reports are sent to the log file.

Generally, -f <filename> is used in conjunction with the -i <n> option (Information detail level). If -i <n> is not specified, the log defaults to -i 0. At this level only virus detections are logged. See the -i <n> option for the Information detail levels. For example:

```
cscmdline -s 192.168.0.100 -f c:\cmdline.log -i 2 c:\winnt
```

The -v option (Verbose mode) can also be used with the -f <filename> option to add virus infection information to the log file. See the -v option for a summary of virus detection information. For example:

```
cscmdline -s 192.168.0.100 -f c:\cmdline.log -v c:\winnt
```

Help display

-h

For a brief summary of command-line options, use the -h option (Help display). For example:

```
cscmdline -h
```

Information detail level

-i <n>

The -i <n> option specifies what to report during processing. The value for <n> is 0, 1, 2, 3, or 4. If -i <n> is omitted, -i 0 level is reported by default.

-i 0 Reports a simple scan summary.

-i 1 Reports viruses detected and viruses that cannot be repaired.

-i 2 Reports which directories were scanned, any errors that occurred, any viruses detected, and any excluded items that were not scanned. See -c <filename> for information about excluded files.

-i 3 Reports which files and directories were scanned, any errors that occurred, any viruses detected, and any excluded items that were not scanned. See -c <filename> for information about excluded files.

-i 4 Reports the current date and time, which files and directories were scanned, any errors that occurred, any viruses detected with the action taken, and information on any viruses detected during the scan. Typically, level 4 is used only for troubleshooting.

For example:

```
cscmdline -s 192.168.0.100 -i 2 c:\winnt
```

The -i <n> option can be used in conjunction with the -f <filename> option (File for logging). As the detail level increases, the log file can grow large. For a scan of 13,500 files, the log might be approximately 50K at the -i 2 level. The same scan at the -i 4 level is about 5 MB.

Located on the CarrierScan Server

-l

The -l option indicates that the files to be scanned are located on the CarrierScan Server itself. Only filenames are passed to the CarrierScan Server, not the files themselves.

If the Symantec AntiVirus Command Line Scanner and the CarrierScan Server are on the same physical computer and the CarrierScan Server is installed on the default port (7777), you can omit the -s <IP address>:<port> option. For example:

```
cscmdline -l c:\file.xyz
```

If the CarrierScan Server is installed on another port, you must specify the -s <IP address>:<port> option. For example:

```
cscmdline -l -s 192.168.0.101:5010 c:\file.zyx
```

If the Symantec AntiVirus Command Line Scanner and the CarrierScan Server are located on the same computer, you can use the trailing * wildcard and the -r option to recurse through subdirectories. See the -r option (Recursive subdirectory scanning) for information. For example:

```
cscmdline -l -r c:\winnt
cscmdline -l -s 192.168.0.101:5010 -r c:\winnt
```

When using the Symantec AntiVirus Command Line Scanner to connect to a remote CarrierScan Server using the -l option, you must use the -s <IP address>[:<port>] option to specify the CarrierScan Server. If the CarrierScan Server is installed on the default port (7777), the :<port> parameter can be omitted. For example:

```
cscmdline -l -s 192.168.0.1 c:\file.xyz
cscmdline -l -s 192.168.0.101:5010 c:\file.zyx
```

When using the -l option to scan files on a remote CarrierScan Server, two restrictions apply:

- Only explicitly named files can be scanned.
- If the CarrierScan Server runs on a different operating system than the computer with the Symantec AntiVirus Command Line Scanner, the file specifications must be in the format of the CarrierScan Server.

Use quotation marks to ensure that the file specification is passed properly. For example, if Symantec AntiVirus Command Line Scanner is running under Windows and the CarrierScan Server is running under Solaris:

```
cscmdline -l -s 192.168.0.1 "/tim/export/jump.cmd"
```

Recursion (-r option), directories, and wildcards are not supported if the CarrierScan Server is located on a different computer. You must specify full paths to explicitly named files for the <path> parameter. There is no mechanism on the CarrierScan Server itself to recurse through directories and the Symantec AntiVirus Command Line Scanner does not include functionality to remotely recurse directories.

Recursive subdirectory scanning

-r

By default, the Symantec AntiVirus Command Line Scanner does not recursively search directories for files to send to the CarrierScan Server. Use the -r option (Recursive subdirectory scanning) to scan descending directories. For example:

```
cscmdline -r -s 192.168.0.105 c:\winnt
```

You cannot use the -r option to scan directories that reside on a remote CarrierScan Server. See the -l option for information.

Server address of CarrierScan Server

-s <IP address>[:<port>]

The -s option can be omitted if the CarrierScan Server is installed on the default port (7777) and on the same computer as Symantec AntiVirus Command Line Scanner. You must specify the IP address and port if the CarrierScan Server is installed on a port other than the default.

If the CarrierScan Server is not located on the same computer as the Symantec AntiVirus Command Line Scanner, you must specify the IP address of the CarrierScan Server. For example:

```
cscmdline -s 192.168.0.100 c:\boot.ini c:\winnt c:\temp
```

If the CarrierScan Server is installed on a different port other than the default (7777), you must specify the port as well. For example:

```
cscmdline -s 192.168.0.100:5010 c:\boot.ini c:\winnt c:\temp
```

Verbose mode if a virus is detected

-v

With the -v option (Verbose mode), virus detections and information about viruses detected are reported. For example:

```
Symantec CarrierScan Version 2.1
Scanning ...
Infected:  CASCADE.COM
Info:      Cascade (1) (Infection was repaired)
Scanning ...
Completed: Scanned: 1  Infected: 1  Repaired: 1
```

The -v option (Verbose mode) output can be directed to a log file with the -f <filename> option.

Configuration file options

By default, the Symantec AntiVirus Command Line Scanner requires a configuration file called cscmdline.cfg in the same directory as the Symantec AntiVirus Command Line Scanner itself. The cscmdline.cfg can be empty, but it must exist. If cscmdline.cfg does not exist, or if you want to use a configuration file with different settings, use the -c option on the command line.

A configuration file can contain two elements:

- Exclude = <path>; [<path>;] ...
- CheckFileHeaders = 0|1

The configuration can contain both, either, or neither of the parameter lines.

Exclude = <path>; [<path>;] ...

To reduce demand on network resources, the configuration file lists files and directories to exclude from scans. Items not at risk of infection can be skipped.

The Exclude = line in the configuration file is a semicolon delimited list of files and directories to exclude from scans. The <path> parameter can be files or directories. For example, the configuration may contain the following:

```
Exclude = c:\pagefile.sys; c:\winnt
```

For all platforms (Windows, Solaris, and Linux), drive letters, filenames, and directory names in the configuration file are case sensitive. The case is determined by how the operating system of the scanned computer returns the filename. For Solaris and Linux, this is usual behavior. Because the Symantec AntiVirus Command Line Scanner is a multi-platform utility, this convention applies to Windows as well.

For example, the following command recursively scans the c:\Program Files directory using the default cscmdline.cfg exclusions file:

```
cscmdline -s 192.168.0.1 -i 2 -r “c:\Program Files”
```

If the cscmdline.cfg contains either of the following lines, the c:\Program Files directory will not be excluded from the scan:

```
Exclude = C:\Program Files;
```

```
Exclude = c:\program files;
```

In the first case, the exclusion fails because the Windows operating system returns the drive letter as lower case. In the second case, the exclusion fails because the Windows operating system returned upper case P and F in the directory name.

CheckFileHeaders = 0|1

The CheckFileHeaders parameter ensures that high risk files are scanned even if they are specified as exclusions. If CheckFileHeaders=1, the Symantec AntiVirus Command Line Scanner reads file headers to determine if it is an executable file. If CheckFileHeaders=0 or the line is omitted, the Exclude list is respected without exception.

For example, if your configuration file contains the following:

```
Exclude = c:\cscmdline.exe
CheckFileHeaders=1
```

And you scan with the following command:

```
cscmdline -s 192.168.0.1 c:\
```

cscmdline.exe is scanned because CheckFileHeaders is set to 1.

SUPPORT

Service and support solutions

Technical support

Symantec offers several technical support options:

- Online Service and Support

  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. This gives you access to current hot topics, knowledge bases, file download pages, multimedia tutorials, contact options, and more.

- PriorityCare telephone support

  PriorityCare fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.

  You can also access the PriorityCare number for your product through the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options available for your product and version.

- Automated fax retrieval

  Use your fax machine to receive general product information, fact sheets, and product upgrade order forms by calling (800) 554-4403. For technical application notes, call (541) 984-2490.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the old version for up to twelve months after the release of the new version. Technical information may still be available through the Service & Support Web site (http://service.symantec.com).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Access customer service options through the Service & Support Web site at http://service.symantec.com. From this site, you can receive assistance with non-technical questions, and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at:
http://www.symantecstore.com

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under the Global Service and Support.

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403
(541) 984-2490

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.service.symantec.com/mx
+54 (11) 5382-3802

Asia/Pacific Rim

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

http://www.service.symantec.com/br
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

http://www.service.symantec.com/mx
+52 (5) 661-6120

Other Latin America

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

http://www.service.symantec.com/mx

Subscription policy

If your Symantec product includes virus, firewall, or web content protection, you might be entitled to receive protection updates via LiveUpdate. The length of the subscription could vary by Symantec product.

When you near the end of your subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your initial subscription ends, you must renew your subscription before you can update your virus, firewall, or web content protection. Without these updates, your vulnerability to attack increases. Renewal subscriptions are available for a nominal charge.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

July 13, 2001

Symantec AntiVirus™ Command Line Scanner
CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name ____

Company Name ____

Street Address (No P.O. Boxes, Please)____

City ______________________________ State _______ Zip/Postal Code ________________

Country* ______________________________ Daytime Phone ______________________________

Software Purchase Date ____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributer.

Briefly describe the problem:____

____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	______
Shipping & Handling	$ 9.95
TOTAL DUE	______

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _________ __ Visa __ Mastercard __ American Express

Credit Card Number ____Expires __________

Name on Card (please print) ______________________________ Signature ______________________________

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003 (800) 441-7234

Please allow 2-3 weeks for delivery within the U.S.